Amendments to the Specification:

A. Please replace the paragraph beginning on page 1, line 5 with the marked-up version below showing the change.

The invention relates to distribution and consumption of documents, and more particularly, to a method and apparatus for controlling various rights in, and access to, the content of documents displayed with the rendering engine of a standard application program, such as an Internet Web Browser.

B. Please replace the paragraph beginning on page 12, line 6 with the marked-up version below showing the change.

Server 220 has a plurality of documents 222 stored thereon, in the form of Web pages, for distribution. Documents 222 can be stored in an encrypted format. The term "encrypted", as used herein, refers to any mechanism by which accessibility of content is partially or completely prohibited, such as by use of asymmetric or symmetric encryption algorithms, scrambling algorithms, or the like. Server 220 also includes rights management module ~~234~~ 224, in the form of software, for storing and managing rights associated with particular ~~ones of~~ documents 222, users, and/or payment amounts as will be described in greater detail below.

C. Please replace the paragraph beginning on page 13, line 21 with the marked-up version below showing the change.

The invention can be implemented in connection with known client/server networking architectures, such as the Web, without modifying, obviating, or bypassing the standard client software, server software, and rendering engines. Rights management module 224 is installed in server 220 along side the existing server software 226. As noted above, rights management module 224 identifies which rights are associated with documents 222 existing on server 220 or later stored on server 222. For example, rights [[. Rights]] management module 224 can have a programmable database, lookup table, or the like including the various rights associated with

each document 222 and other variables, such as the identity of the user and the payment made by the user, in a well known manner. Rights management module 224 further interfaces with the operating system API of server 220 to cause server software 226 to only respond to connections from client(s) 230 having connection module 236 and UI module 234. In particular, once rights management module ~~234~~ 224 is installed, the procedure illustrated in Fig. 3 is accomplished. In step A, a new DRM start Web page, or other secure interface display, is created which references UI module 234 and the existing server start Web page. In step B, the various Web pages of a Web site on server 220 can be placed in a directory having a random label or any unknown directory. In step C, rights management module 224 is programmed to include a pointer to this directory, and, in step D, rights management module 224 encrypts the URL of this directory. In step E, the start DRM Web page is modified to reference UI module 235 which can instruct connection module 236 to unencrypt the encrypted URL to permit access to original start page and to the rest of the Web site. If client 230 does not have UI module 234 and connection module 236, the URL cannot be unecrypted and thus the Web site on server 220 cannot be accessed.